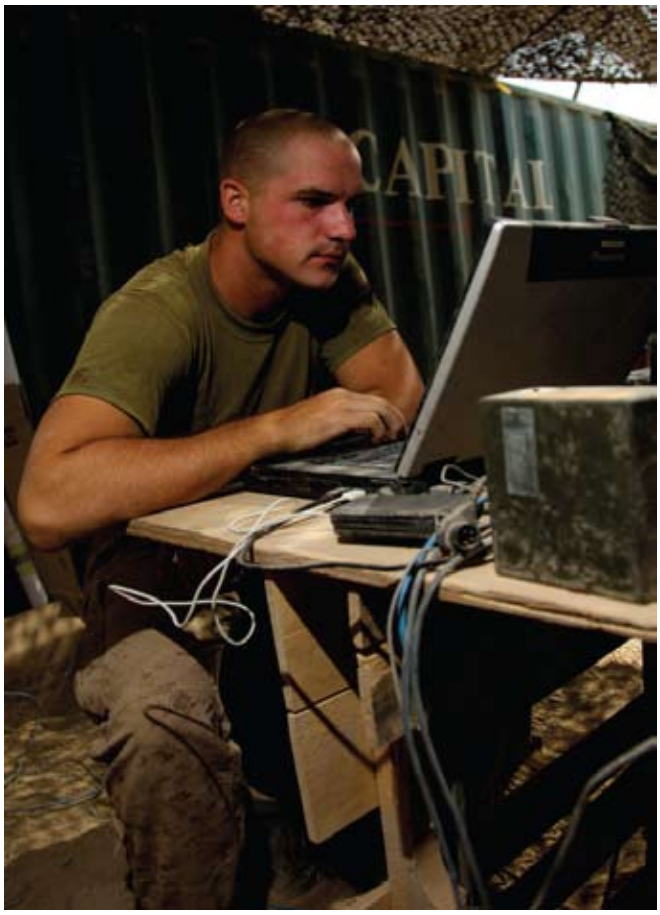
The Dark Side of Social Networking

by
Mike McGannon and Dr. David Hurley, PhD

Editor's Note: Mr. McGannon's and Dr. Hurley's views on social networking and the possibilities of unwarranted disclosure are pertinent and relevant to operations security concerns of all organizations. This article provides a relevant perspective for that point of view.

The 1990s saw access to the Internet rise from the computer scientist and hacker realm to a common household service such as cable television and telephone services. In the first decade of the 21st century with the advent of more powerful smart phones, PDAs and netbooks, and high speed Internet services, online access can be achieved by anyone, anytime even in the most remote locations in the world. For this new generation of users who have always had Internet access, a new form of website has come on the scene: the social networking website a cross between the old bulletin board services, weblogs (blogs), fan pages and instant message services. These websites offer the latest in web 2.0 technology and allow users to broadcast their every interest and most minute detail about their lives across to their networks of friends. These advances in technology have changed interpersonal communication and the manner in which people socialize.



US Marine Using Tactical Computer
Source: defenseimagery.mil

The upside to these websites for users is that they are fun while still offering a means to communicate with their friends and offer the ability to share photos, videos, links, RSS feeds, games, and other applications. Literally individuals through online technology can be interconnected worldwide. While individuals are no longer geographically bound in their communication and socialization, these new freedoms bring new dangers, with a hazardous downside, for those users who are also in or support the military and the intelligence community. The rapid expansion in the number and sophistication of social networking websites and blogs in the online community, coupled with a dramatic increase in the number of personnel participating on these websites, have increased the need for focused Operations Security (OPSEC) awareness. According to news reports our adversaries are quite proficient in the use of online tools and research methods. They are cognizant of the intelligence bonanza to be reaped through exploitation of unclassified online source.[1,2] They also are adept at employing the Internet as a communications medium. The free flow of personal information that is often posted on these websites may be of interest to adversaries of the United States and all too frequently the posted information is in violation of standard OPSEC rules and regulations. Moreover, imprudent use of social networking websites makes the unwary user vulnerable to Cyber Threats, Adversary Influence Operations, and Foreign Intelligence Services who may be using these websites to gather information or to target United States personnel…hence the dark side of online social networking.

In 2007, the Air Force Research Lab Human Effectiveness Directorate Special Projects office published the report "The Impact of Internet Social Networking on the Vulnerability of United States Air Force Personnel to Adversary Influence Operations." The purpose of the study was to examine the potential vulnerability that Untied States Air Force (USAF) personnel may incur through their online social networking behavior.

The research team collected a data sample from 500 MySpace® profiles and several findings stood out: according to the study, 60.4% of USAF personnel posting on MySpace® supplied enough personal details to make themselves vulnerable to adversary targeting. Their MySpace® pages included critical information such as first name, last name, hometown, home state, duty location, and job type.[3] Of the remaining posters, 25.4% were found to be fair targets, and only 14.2%

were found to be poor targets. Also, the study concluded that age is the variable most highly correlated with a propensity to post personal information on MySpace®. Approximately 68% of the USAF MySpace® postings were done by individuals under the age of 26. Approximately 90% of USAF MySpace® posters were under 30 years old. Variables highly correlated with age, such as marital status (unmarried) and rank (lower enlisted and company grade officers), also proved to be significant indicators.The enormity of this problem should not be understated. The significance of the age variable goes much deeper than highlighting the imprudence of youth. Simply put, we do not expect large numbers of individuals to age out of this behavior because the age variable seems less an indicator of youth and more of a gauge to their generation. As this younger tech savvy cohort matures, they bring with them new manners of socializing and communicating based on technology unavailable to previous generations. Hence, as this generation of USAF personnel matures, we would expect the age variable to increase as well, meaning over time we only expect this problem to grow.

Why Users are Vulnerable

The problem goes beyond just the seven critical variables identified in the study, users are also able to post as much or as little information as they choose to in the general profile fields. When these fields are completely filled in, they provide even more details for an adversary to target the online poster. This is an additional adversary benefit, because they have a baseline via social networking to contact and solicit additional information from the user, their friends, or family members. This information can be crosschecked by conducting more detailed searches of public records information and for initiating professional (charge-for-service) background checks. Because the profiles also list friends of the user, the potential adversary obtains another avenue through which to gather information and perhaps additional targets. The following are examples from a MySpace® profile, but most of the major social networking websites have the same general categories.

Interest and Personality Section

Social networking website users generally provide lengthy and often very detailed information about themselves in the Interest & Personality section. While the user may believe this information to be innocuous, it is exactly the type of information that an adversary can leverage for use in Influence Operations planning, with the user as the primary target. Persons with whom the primary target has relationships with are also imperiled by this information if it is posted and freely shared on the site.

Privacy Act Information

Personal information that is covered by the Privacy Act, such as full name, date of birth, hometown, and address, is of particular value to an adversary. Such information can form the basis of a pay-for-service record/background check and each iteration can provide increasingly more detailed information suitable for refining a target folder, as well as for identify theft.

Military Information

Social networking website users should never provide sensitive, but unclassified, military information on their websites. Sensitive military information includes current duty station, current organization, occupational specialty (especially such sensitive specialties as: security forces, intelligence, nuclear weapons, aviation career fields, etc.), deployment location, and ongoing or future operations. Indeed, any information that would be covered in an OPSEC briefing should not be posted on a website or online profile where it can be accessed by the general public.

Lifestyle Information

Lifestyle details can be an adversarial point of influence if a user has posted information that he or she has not or cannot divulge to superiors, coworkers, and friends. Such information includes homosexual orientation, illegal drug use, and similar data. Users should be aware that being online does not mean that one is anonymous. As the recent troubles of Olympian Michael Phelps can attest, even photos can be compromising to one's image and financial opportunities.

Education and Employment

Educational and employment information can be valuable to an adversary because it provides yet another avenue to obtain desired details about a target's life. Targeteers can use such information to gain additional data via second-tier individuals identified through such sources such as alumni magazines and company websites.

OPSEC Implications

There are many OPSEC implications with regards to social networking websites and while there is no harm in using these websites, users do need to be aware of what they should and should not be posting about themselves, their duty station, and their operations. Users should always refer to their specific organization's OPSEC regulations if they are unsure of what information they can talk about in a public forum, however, as a general rule they should keep in mind that critical information that constitutes what the adversary needs to know about an organization's operations or programs to achieve their goals. Users should always ask themselves when creating or updating their profile information "Could this information be exploited by an adversary in any way or pieced together with other information?" While the individual user may not post detailed information about themselves, their friends or family members who are linked to their profile may be posting every little detail about their lives. Users should never underestimate the capabilities or conviction of our adversaries when it comes to collecting information on their targets.

The Counter Intelligence Problem

There is a common misconception that counter intelligence deals with spies collecting information on other spies and this is simply not the case. Adversaries of the United States, both traditional and

emerging threats (terrorist organizations, non-state actors, etc.), will use the best collection tools at their disposal to gather information. Everyone has the ability to access the Internet and social networking websites, so it is a reasonable assumption that users on these websites could become the target of overt or even covert collections by a foreign entity.

Cyber Threats

Once an adversary has collected enough information on a target they may choose to carry out some form of cyber attack against the individual, which could include identity theft, viruses or other malware, or even Influence Operations. Social networking websites lend themselves to such cyber attacks because users are lulled into a false sense of security and do not think that any of the applications or other tools they are using on the website pose a threat. Adversaries could easily create applications to harvest information, install malware or simply monitor the user. In the realm of Influence Operations, an adversary is likely to employ robust means of influence that are not restricted by official doctrine or rules of engagement. For example, the toolkit of adversarial influence methods may include bribery, criminal acts, blackmail, humiliation, kidnapping, and harm or threat of harm—both to the primary target and/or their loved ones.

Conclusion

The use of social networking websites as a tool will only increase as web and mobile computing technologies evolve and while the new generation of soldiers, sailors, airmen and marines enter the service with the web presence in tow, they need to be made aware of the implications that using these websites have on their careers and how they can affect their unit's operations.

Footnotes:

1 Chris Fowler, 24 April 2007, "Posting Online Videos Can Be Boom or Bust for U.S. Service Members," Stars and Stripes [Internet, WWW]. Available: 529 14th St NW, Washington, DC 20045 ADDRESS: http://stripes.com/article.asp?section=104&article=52866&archive=true, [Accessed: 24 June 2007].

2 Alexis Debat, 10 March 2006, "Al Qaeda's Web of Terror," ABC News [Internet, WWW], Available: ABC NEWS INC., 47 W 66TH ST #800, New York, NY, 10023, ADDRESS: http://abcnews.go.com/Technology/Story?id=1706430&page=1, [Accessed: 24 June 2007].

3 The study found that these seven variables were the key ones to track and locate an individual. How much information individuals voluntarily provided on these seven critical pieces of information determined the easy and probability of finding them. Individual providing between 0-3 of the critical variables were found to be poor targets, due to the lack information needed for targeting efforts. While individuals providing 4-5 critical variables were categorized as fair targets because they able to be targeted some of the time, and those posting 6-7 variables were categorized as good targets because their targetability was high.